ThoughtWorks® presents:

Agile Threat Modelling

Katharina Dankert

Jennifer Parak

Michael Lihs

Speakers

Katharina Dankert
@yuiofthesun

Jennifer Parak
@jenpaff

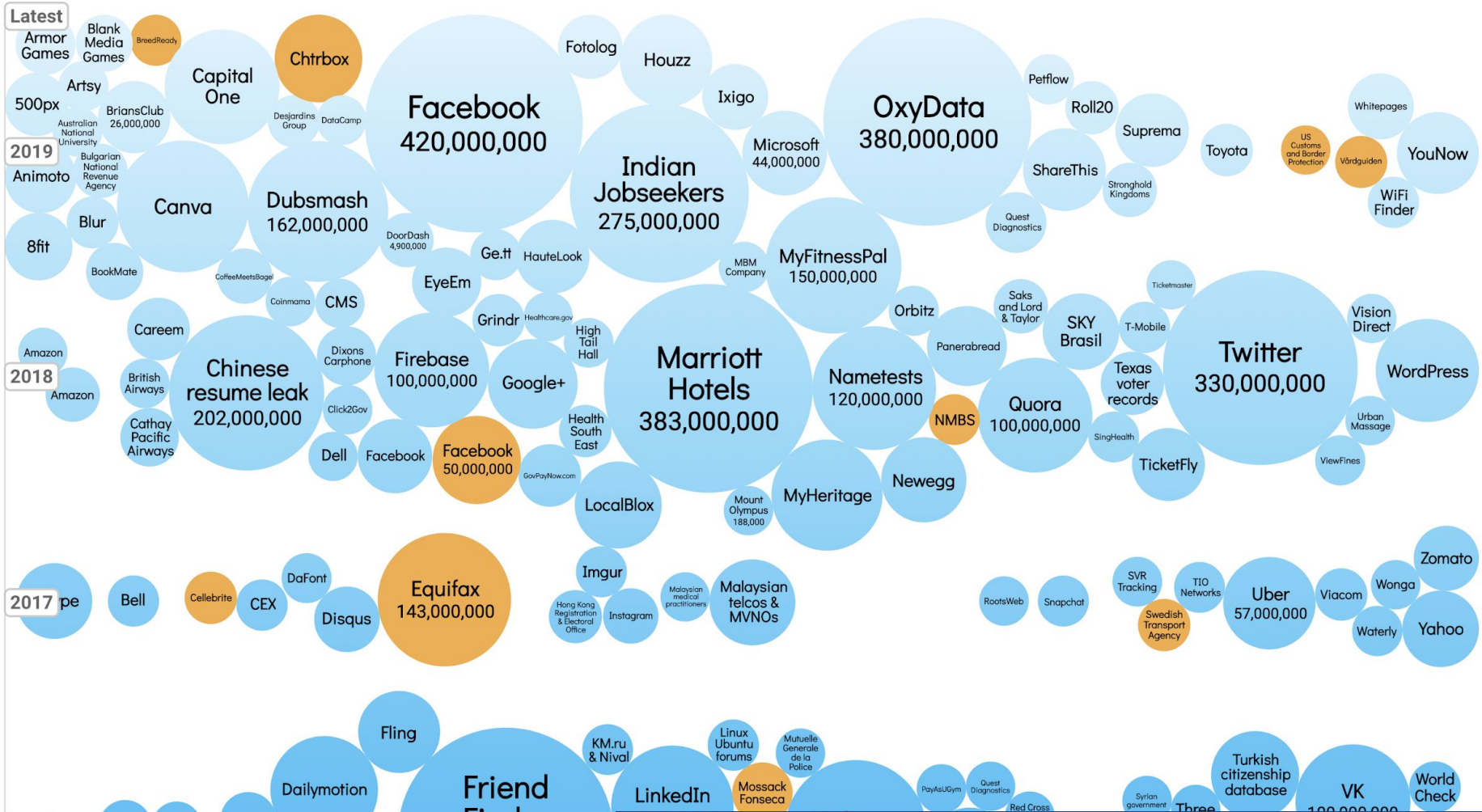
Michael Lihs
@kaktusmimi

Agenda

- Motivation
- Theoretical Part
- Practical Part
- Summary

photo from unsplash

Motivation



www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ [2020-01-13]

Agile Software Development

vs

Security ?

photo from unsplash

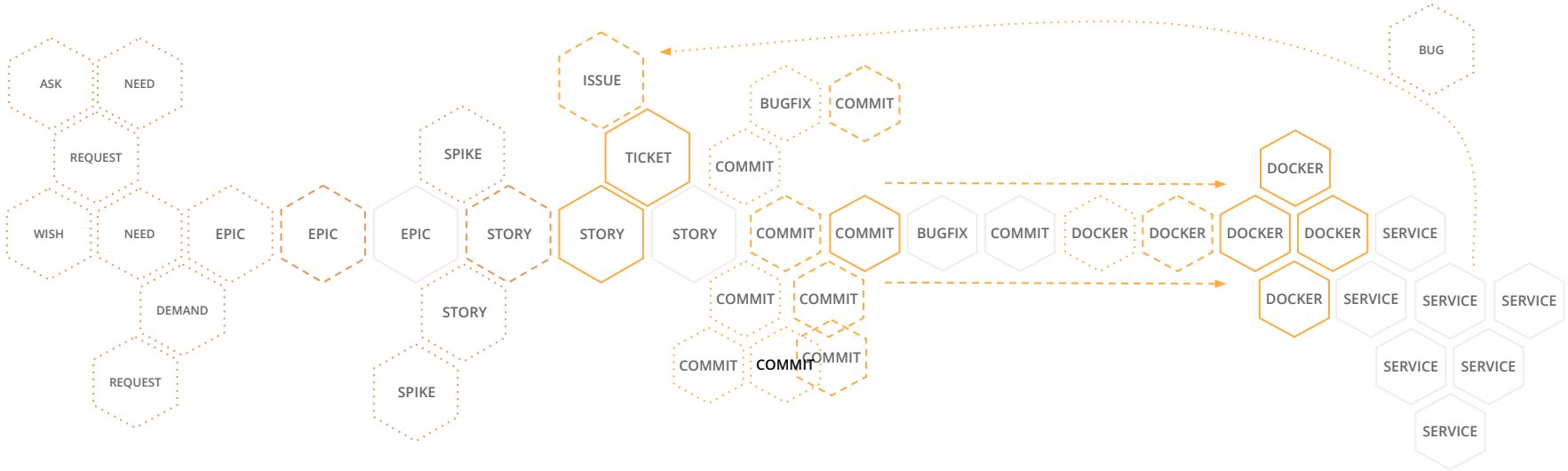
Traditional threat modelling - security sandwich

- Often seen by devs as externally imposed
- Cannot capture changing state of system

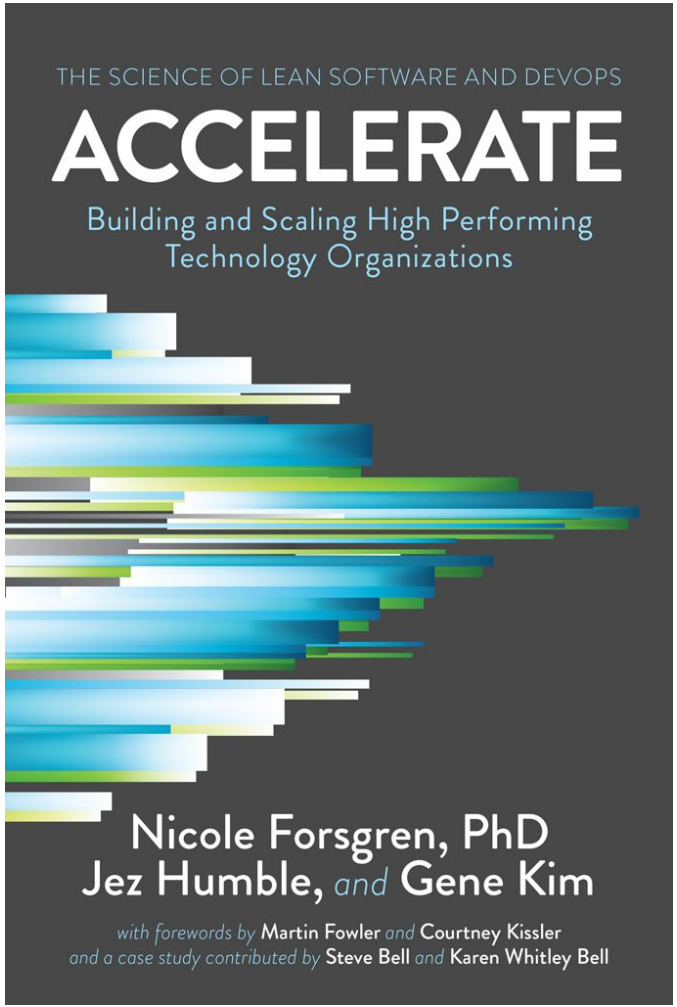
Photo by Valeria Boltneva from Pexels

Shift-left on Security

Path to Production



Inspired by Felix Hammerl



"High-performing teams spend 50 percent less time remediating security issues than low-performing teams."

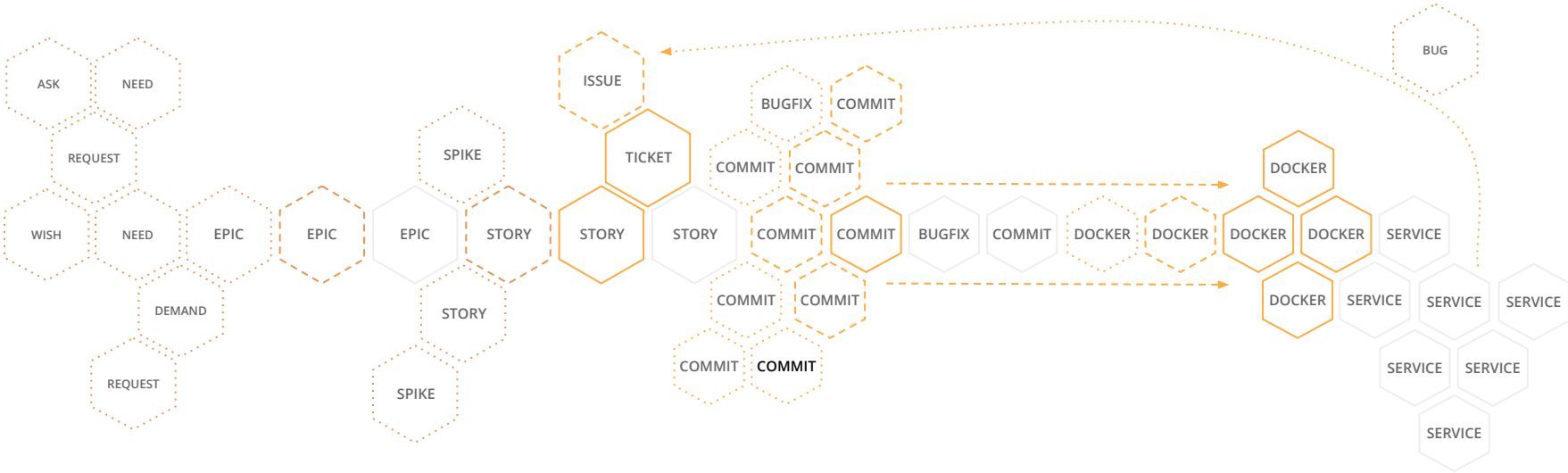
State of DevOps Report, 2016

What is threat modelling?

Photo by Dan Gold on Unsplash

Questions?

photo from unsplash



Discussions
Verbalization of functionality

Requirements
Molding needs into epics

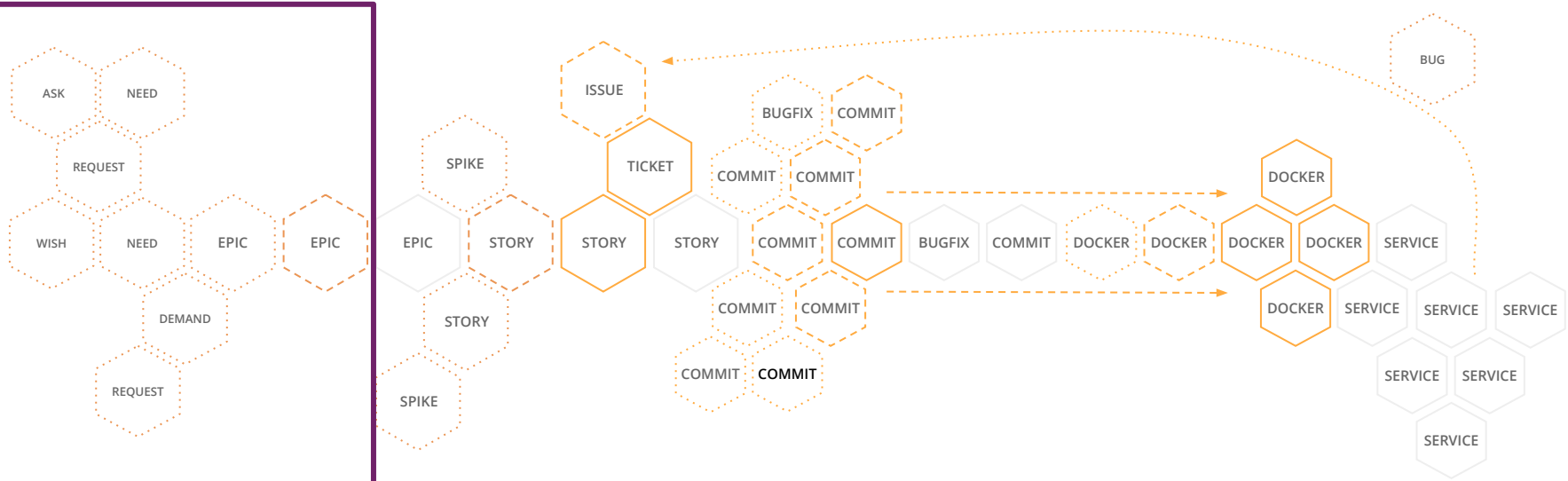
Analysis
Breaking down epics into stories

Development
Where stories become deliverables

QA
Where deliverables are reviewed

Deployment
Deliverables become functionality

Slide by Felix Hammerl



DESIGN

Agile Threat Modelling

CODE

Static Code Analysis...

INHERIT

Credential Scanners...

BUILD & TEST

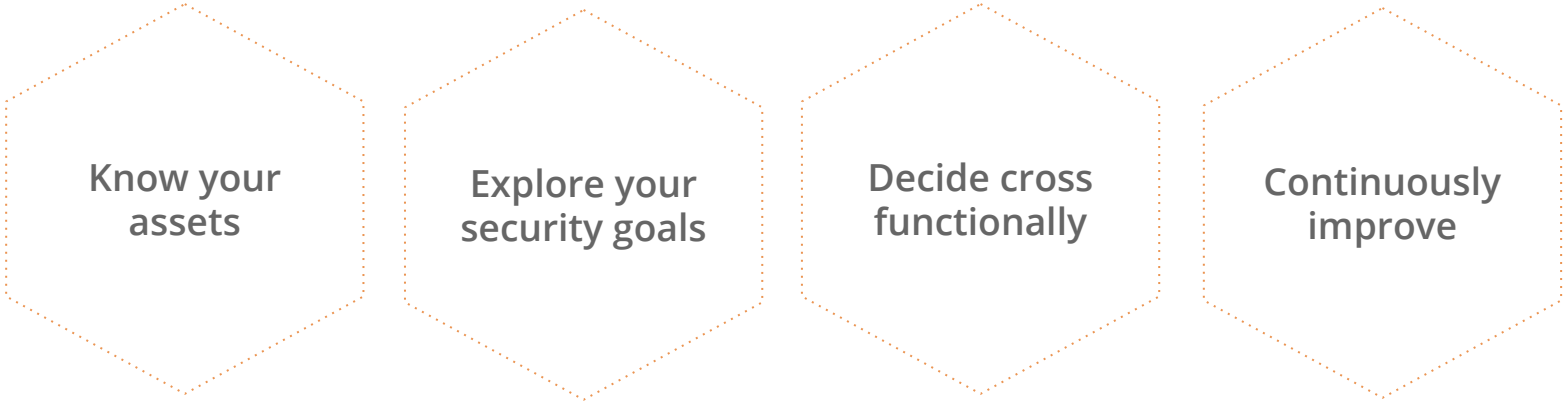
Vulnerability Scanners...

DEPLOY

Secure Pipelines...

OPERATE

Monitoring & Alerting...



DESIGN

Having a threat model document

Continuously practising threat-modelling

Not mutually exclusive

photo from unsplash

What are assets?

Valuable goods of **physical** or **immaterial** nature that have value for both the organization and the attacker.

Targets for both **deliberate** and **negligent** threats.

Think in terms of **business goals** rather than purely technical assets.

What are security goals?

Assets have **security goals** that often derive from business/legal/regulatory requirements.

These security goals being broken results in a **disaster scenario**, which carries an impact to your business.

Asset library

Asset	How bad would be if we violated...		
	Confidentiality	Integrity	Availability
User emails	Possible legal issues Loss of trust	Service disruption Loss of trust	Service disruption Loss of trust
User shipping address	Likely legal issues Loss of trust	Incorrect deliveries Loss of trust	Service disruption Loss of trust
Bike prices	No impact (already public)	Incorrect billing	Can't place orders Loss of revenue
Legal docs (T&Cs)	No impact (already public)	Possible legal issues	Possible legal issues

Agile **Threat Modeling**

Scope → **Architecture, Network, Boundaries** → **Investigate** → **Prioritize**

You are looking for a **realistic** scope for a 1-hour session.

Draw your **relevant** components, data flows, interactions, and system/network boundaries.

Use evil-brainstorming techniques (e.g. STRIDE cards) to **drill down**.

Align on the x **most valuable items**. Enrich into proper stories. Add to sprint backlog.

Follow up - **Dealing with risk**

Mitigate?	Identify? Protect? Detect? Respond? Recover?
Transfer?	To whom?
Avoid?	What are the alternatives?
Accept?	Keep a record of the security debt!

Questions?

photo from unsplash

Running a Threat Modelling Workshop

A working example

Questions?

photo from unsplash

Agile Threat Modelling is a journey...

Assets & security objectives

Threat model little and often

Per story

Agile

Exploratory

Agile Threat Modelling Workshop

What are we building?

What can go wrong?

What are we going to about it?

Create a Community

Design

Threat Model often

Shift security **left**

Enable the delivery **teams**

Code

Apply controls on **hardware**

Prevent leaking **credentials**

Static **code** analysis

Inherit

Check for vulnerable **dependencies** continuously

Update simple and often

Reduce **noise**

Build & Test

Test your **security assumptions**

Automate attacks

Deploy

Rebuild your infra often (and scripted)

Scan and **patch** vulnerabilities in infra

Segregate environments

Operate

Monitor and understand your **real threats**

Append only **logs**

Run and automate **disaster recovery**

Further Resources

- Article on Agile Threat Modelling by Jim Gumbley
- Accelerate by Nicole Forsgren, Jez Humble, Gene Kim
- S.T.R.I.D.E cards attached

Thank you

Katharina Dankert
katharina.dankert@thoughtworks.com

Jennifer Parak
jennifer.parak@thoughtworks.com

Michael Lihs
michael.lihs@thoughtworks.com

ThoughtWorks® */careers*